МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІВЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені Юрія Федьковича
Навчально-науковий інститут фізико-технічних та комп'ютерних наук

Кафедра радіотехніки та інформаційної безпеки

ЗАТВЕРДЖУЮ

Ректор _____ Роман ПЕТРИШИН

«__» _____ квітня _____ 2024 р.

ПРОГРАМА ВСТУПНОГО КОМПЛЕКСНОГО ФАХОВОГО ІСПИТУ

на навчання за другим (магістрським) рівнем вищої освіти
на базі рівня вищої освіти бакалавр

Спеціальність ***125 Кібербезпека та захист інформації***
(шифр і назва спеціальності)

Освітньо-професійна програма ***Кібербезпека***
(назва ОП)

Схвалено
Вченою радою ННІФТКН
протокол №4 від 18.04.2024 р.

Голова Вченої ради Олег АНГЕЛЬСЬКИЙ

Чернівці, 2024 р.

1. Лінійні блокові систематичні коди, генеруюча та перевіркова матриця.
2. Характеристики мовних сигналів.
3. Основні методи закриття мовної інформації.
4. Циклічні коди.
5. Методи вимірювання акустичних параметрів.
6. Аналогові скремблери: класифікація та принцип дії.
7. Згорткові коди.
8. Акустичні вимірювальні перетворювачі.
9. Цифрові скремблери: класифікація та принцип дії.
10. Імпульсно-кодова модуляція.
11. Ентропія дискретного джерела повідомлень. Умовна та сумісна ентропія зв'язаних джерел повідомлень.
12. Власна інформація повідомлень.
13. Сумісна та взаємна інформація повідомлень.
14. Взаємна інформація зв'язаних каналом джерел повідомлень. Кількість інформації, що передається по каналу зв'язку.
15. Загальні принципи акустичних перетворювачів. Механічні та електричні аналогії в акустиці.
16. Акустоелектроніка. П'єзоелектричні резонатори. Пристрої на поверхневих акустичних хвилях.
17. Імпульсна та перехідна характеристики лінійних дискретних систем.
18. Види ліній зв'язку та їх основні характеристики.
19. Властивості лінійних дискретних систем.
20. Первинні та вторинні параметри ліній зв'язку.
21. Генератори з зовнішнім збудженням.
22. Пряме та обернене перетворення Фур'є для дискретних сигналів.
23. Поверхневий ефект в лініях зв'язку. Причина явища.
24. Види і природа виникнення каналів витоку інформації при експлуатації ЕОМ.
25. Властивості z-перетворень.
26. Ефект близькості (зближення) в лініях зв'язку. Причина явища.
27. Джерела утворення радіоканалів витоку інформації.
28. Передавальна функція лінійних дискретних систем.
29. Конструктивні елементи кабелів зв'язку.
30. Класифікація технічних каналів витоку інформації.
31. Основні класи симетричних криптосистем.
32. Принцип дії пасивного інфрачервоного датчика руху.

33. Модель криптосистеми з відкритим ключем.
34. Загальна модель системи захисту об’єкту.
35. Шифр Віженера.
36. Типи датчиків, які використовуються в системі протипожежного захисту.
37. Шифр Хілла.
38. Класифікація протикрадіжкових систем захисту.
39. Поліграмні шифри.
40. Основні складові базової системи відеоспостереження.
41. Алгоритм шифрування DES (Data Encryption Standard).
42. Абсолютна і відносна похибки вимірювання. Приведена похибка. Систематичні і випадкові похибки.
43. Криптосистема RSA (Ronald Linn Rivest, Adi Shamir, Leonard Adleman).
44. Криптосистема Ель-Гамаля.
45. Криптосистема Рабіна.
46. Поняття про цифровий підпис.
47. Централізована й децентралізована обробка інформації в інформаційно-вимірювальних комплексах.
48. Нормальний закон розподілу випадкової похибки. Середньо-квадратичне значення та дисперсія випадкової похибки.
49. Структура електромагнітного поля та принципи екранування.
50. Мостовий метод вимірювання параметрів. Повне рівняння балансу моста. Схеми вимірювання R, C, L, Q, tgδ.
51. Динамічні системи, умова стійкості.
52. Будова систем цифрової обробки сигналів.
53. Побічні випромінювання. Електромагнітне екранування.
54. Способи вимірювання частоти. Вимірювання частоти і часових інтервалів методом калібровочних міток.
55. Етапи перетворення аналогового сигналу в цифровий.
56. Стеки. Типи стеків, призначення.
57. Типи архітектур мікропроцесорних систем.
58. Гарвардська та Прінстонська архітектури мікропроцесорних систем.
59. Канали зв’язку в інформаційно- вимірювальних системах.
60. Послідовність операцій аналогово-цифрового перетворення сигналів.
61. Шуми антен. Формула Найквіста для антен.
62. Дискретизація сигналу по часу. Дискретний сигнал. Квантований сигнал. Цифровий сигнал.
63. Різновиди інформаційно-вимірювальних систем.

64. Криптографічні хеш-функції.
65. Види і склад інформаційно-вимірювальних комплексів.
66. Повітряні та екрановані фідерні лінії.
67. Синхронний і асинхронний режими організації передавання.
68. Код Хаффмена. Кодове дерево.
69. Словникові методи кодування. Метод Зіва-Лемпела.
70. Матричні шифри.
71. Алгебраїчна модель шифру гамування.
72. Поточний шифр RC4.
73. Поточний шифр A5.
74. Державна, військова, комерційна і приватна конфіденційна інформація.
75. Перехоплення акустичної інформації за допомогою радіопередаючих засобів.
76. Напрямлені мікрофони. Лазерні системи контролю віконного скла.
77. Типи модуляції сигналу в охоронних системах.
78. Функції державної системи по забезпеченню інформаційної безпеки.
79. Поняття алгоритму. Лінійні, розгалужені і циклічні алгоритми.
80. Алгоритми сортування. Сортування включенням. Сортування злиттям.
81. Принцип побудови і архітектура ПК.
82. Призначення області записування та основи класифікації систем запису та відтворення інформації.
83. Оптичний запис інформації.
84. Методика магнітного запису інформації.
85. Державна, військова, комерційна і приватна конфіденційна інформація. Основні визначення та поняття згідно нормативних документів. Правовий, організаційний і технічний захист інформації. Нормативні документи.
86. Загальна класифікація технічних каналів витоку інформації, яка оброблюється технічними засобами прийому, обробки, зберігання і передачі інформації (ТЗПІ).
87. Забезпечення захисту інформації від ненавмисної дії технічними засобами.
88. Класифікація візуально-оптичних та матеріально-речовинних каналів витоку інформації.
89. Способи і методи захисту інформації (ЗІ, що обробляється засобами електронної техніки, від витоку по радіотехнічному каналу).
90. Технічна реалізація пристроїв маскування.
91. Методи і засоби несанкціонованого отримання інформації по технічних каналах.
92. Методи і засоби несанкціонованого отримання інформації з автоматизованих систем (АС). Методи і засоби руйнування інформації в АС.

93. Основні методи закриття мовної інформації. Аналогові та цифрові скремблери: класифікація, принцип дії.

94. Основні підходи до створення комплексної системи запису інформації.

95. Загальна характеристика мікроелектроніки. Основні терміни і поняття, показники і фактори, що визначають сучасний розвиток мікроелектроніки. Класифікація елементної бази РЕЗ.

96. Виявлення повної множини загроз безпеки інформаційним ресурсам, які підлягають захисту.

97. Проведення оцінки уразливості і ризиків для інформаційних ресурсів, що підлягають захисту, при виявленій множині загроз.

98. Захист інформації в комп'ютерних системах від несанкціонованого доступу.

99. Політика інформаційної безпеки.

100. Впровадження, визначення якості і управління системою захисту інформації.

101. Інформаційна система як об’єкт захисту. Атаки на інформаційні ресурси системи.

102. Організація системи доступу до баз даних. Сучасні систем серверної взаємодії.

103. Організація множинного доступу до інформаційних ресурсів.

104. Особливості передачі інформації в бездротових мережах. Завадостійкі способи кодування в каналах безпровідного зв’язку.

105. Особливості передачі інформації в мережах стільникового та супутникового зв’язку.

106. Захист програмного забезпечення. Класифікація загроз. Класифікація комп’ютерних вірусів.

107. Методи та засоби захисту програмного забезпечення. Методи боротьби з вірусами.

108. Захист програмного забезпечення від реасемблерів та налагоджувачів. Системний підхід до захисту ПЗ.

109. Безпека інформаційних ресурсів у інформаційно-телекомунікаційних системах. Організація технічного захисту інформації.

110. Захист інформації на базі ISO/IEC.

111. Управління доступом і забезпечення цілісності програмного забезпечення.

112. Державні стандарти України в галузі кібербезпеки.

113. Законодавча та нормативно-правова база України в галузі інформаційної та кібербезпеки.

114. Мережева модель OSI. Основні протоколи стеку TCP/IP.

115. Механізми безпеки комп'ютерних мереж.

СПИСОК ЛІТЕРАТУРИ

Основна

1. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів закладів вищої освіти. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ - 2000», 2024 . – 678 с.
2. Інформаційна безпека. Навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик. Львів : Видавництво Львівської політехніки, 2019. – 580 с.
3. Смірнов О.А. Вступ до кібербезпеки: навч. посіб. / Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. – Кропивницький: ЦНТУ, 2022. – 967 с.
4. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак – К.: Видавництво НА СБ України, 2020. – 256 с.
5. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник] / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа: Львів: «Магнолія 2006», 2018. – 320 с.
6. Кібербезпека в Україні: нормативна база, коментарі та роз'яснення, актуальна судова практика, Пєтков С.В., Журавльов Д.В., Дрозд О.Ю., Дрозд В.Г. -К: Видавництво ЦУЛ, 2022. – 460 с.
7. Богуш В.М., Кудін А.М. Моніторинг і аудит систем інформаційної безпеки. К.: ДУІКТ, 2006, – 340 с.
8. ДСТУ EN ISO/IEC 27001:2022 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (EN ISO/IEC 27001:2017, IDT; ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015, IDT).
9. ДСТУ EN ISO/IEC 27002:2024 Інформаційна безпека, кібербезпека та захист конфіденційності. Заходи забезпечення інформаційної безпеки (EN ISO/IEC 27002:2022, IDT; ISO/IEC 27002:2022, IDT).
10. Конституція України / Верховна Рада України. – Офіц. вид. – К.: Відомості Верховної Ради України, 1996. – No 30. – Ст. 141.
11. Закон України «Про інформацію» (02.10.2002 р. No 2657 – XII).
12. Закон України «Про державну таємницю» (21.09.1999 р. No 1079 – XIV).
13. Закон України «Про захист інформації в інформаційно - телекомунікаційних системах» (05.10.1994 р. No 80/94 – ВР).
14. Закон України «Про надзвичайний стан» (26.06.1992 р. No 2501 - XI I).
15. Кримінальний кодекс України (05.04.2001 р. No 2341 – III).
16. Цивільний процесуальний кодекс України (18.03.2004 р. No 1618 – IV).
17. Базові поняття. Терміни та визначення : ДСТУ 2392 - 94. – [Чинний від 01 – 01 – 1995]. – К. : Держстандарт України, 1994. – IV. 89 с. – (Державний стандарт України).

18. Технічний захист інформації. Основні положення : ДСТУ 3396.0 - 96. – [Чинний від 1997 – 01 – 01]. – К.: Держстандарт України, 1995. – IV. 8 с. (Державний стандарт України).
19. Технічний захист інформації. Порядок проведення робіт : ДС ТУ 3396.1 - 96. – [Чинний від 1997 – 01 – 07]. – К.: Держстандарт України, 1995. – IV. 11 с. (Державний стандарт України).
20. Технічний захист інформації. Терміни та визначення : ДСТУ 3396.2 - 97 – [Чинний від 1998 – 01 – 01]. – К.: Держстандарт України, 1995 . – IV. 12 с. (Державний стандарт України).
21. Процеси життєвого циклу програмного забезпечення (ISO/IEC 12207: 1995) : ДСТУ 3918 - 1999 – [Чинний від 2000 - 07 - 01]. – К. : Держстандарт України, 2000. VI. 49 с. (Державний стандарт України).
22. Нормативне забезпечення інформаційної безпеки / [Головань С. М., Петров О. С., Хорошко В. О. та ін.]. – К. : Державний університет інформаційно - комунікаційних технологій, 2008. – 533 с.
23. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1 - 002 - 99. – Офіц. вид. – К. : НікС : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. – III. 15 с. (Нормативний документ системи технічно го захисту інформації).
24. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1. - 003 - 99. – Офіц. вид. – К. : НікС : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. – III. 24 с. (Нормативний документ системи технічного захисту інформації).
25. Типове положення про службу захисту інформації в автоматизованій системі : НД ТЗІ 1.4 - 001 - 2000. – Офіц. вид. – К. : НікС : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. – III. 20 с. (Нормативний документ системи технічного захисту інформації).
26. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 : НД ТЗІ 2.5 - 008 - 2002. – Офіц. вид. – К. : НікС : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2002. – III. 25 с. (Нормативний документ системи технічного захисту інформації).
27. Головань С. М. Вимоги до побудови моделі загроз інформаційних систем / С. М. Головань // Інформаційна безпека – 2009. – No 2 (2) – С. 77 – 84.
28. Несанкціоноване використання інформації та відповідальність за ці дії / С. М. Головань, А. М. Давиденко, О. О. Мелешко [та ін.] // Моделювання та інформаційні технології. Зб. наук. праць Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України. – 2005. – Вип. 35. – С. 3 – 7.

29. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний підручник. Харків, ХНУРЕ, 2011 р.
30. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний конспект лекцій. Харків, ХНУРЕ, 2011 р.
31. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004. – 368 с.

Додаткова

1. Васильєва Л.Д.. Напівпровідникові прилади : підруч. / Л.Д. Васильєва, Б.І. Медведенко, Ю.І .Якименко. – К. : Політехніка, 2003.
2. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мережі. – К.: Самміт-книга, 2010.
3. Задірака В. Комп'ютерна криптологія. Підручник. К, 2002. – 504 с.
4. Радіотехніка № 114, 119, 126, 134, 141, 142,145. Всеукраїнський міжвідомчий збірник.Харків, ХНУРЕ, 2000 - 2008 рр.

Критерії оцінювання результатів вступного фахового іспиту (тестування)

Тест складається з 20 завдань.

За кожну правильну відповідь нараховується 6 балів. Загальна оцінка за тест дорівнює сумі набраних балів, збільшеній на 80 балів. Отриманий результат знаходиться в межах від 80 до 200 балів.

Для допуску до участі в конкурсі на фаховому вступному випробуванні потрібно отримати не менше 100 балів.